Health Claims for Auto Insurance

INSURER USER MANUAL

Chapter 11

Security & Privacy

June 2014

Chapter 11: Security & Privacy

Overview

This chapter discusses security and privacy in the HCAI system.

Privacy and Security in HCAI 2
Secure Hosting Facility 2
User Authentication 2
Application Log-in 2
Client Digital Certificates 2
Client Digital Certificates 3
Web Services Authentication Errors 3
Authorization Configuration 4
Auditing 5
Audit Data Retrieval 5
Archiving 5
Privacy Practices 6

Privacy and Security in HCAI

The Personal Information Protection and Electronic Documents Act (PIPEDA) and the Ontario Personal Health Information Protection Act (PHIPA) legislate how organizations that hold personally identifiable information (PII) must operate. Both acts describe how organizations are to collect, use, and disclose information. Further, they determine that all PII must be:

- accurate;
- stored in a secure manner;
- accessible for inspection and correction purposes;
- collected with consent and for a purpose that is reasonable; and
- disclosed and used for the purpose for which it was obtained

HCAI is subject to the requirements set down by PIPEDA. Because quality data is a precious resource, HCAI employs multiple technologies and security practices to ensure the protection of the data entrusted to it, as described below.

Security

Secure Hosting Facility

The HCAI infrastructure is housed in secure hosting facility and access is restricted to authorized personnel for the purposes of maintaining the system and that access is logged.

User Authentication

HCAI has been designed so that only authorized Users can access information in the system. HCAI uses two mechanisms to confirm the identity of its Users: application log-in and digital certificates.

Application Log-in

All Users must enter a valid User Name and password to log in to the HCAI system. To maximize the security of every password, HCAI requires that they must:

- contain at least six characters;
- contain at least one character from three of the following four groups:
    - uppercase characters
    - lowercase characters
    - numerals
    - symbols (characters not defined as letters or numerals such as @, !, #, and so forth);
    - not contain the User's actual name, User name, or either of these spelled backwards; and
- be changed every 90 days.
- As an additional security measure, if a User fails to provide the valid password for the same User name 5 times, the User suspended. Only an HCAI Administrator can reset the password once the password has been suspended.

Client Digital Certificates

Digital certificates are electronic credentials that connect the identity of the certificate owner to a pair (public and private) of electronic keys that can be used to sign information digitally. These electronic credentials make sure that the keys actually belong to the person or organization specified.

HCAI integration Web services (such as data feeds, and data extractions) use digital certificates for authentication of remote machines. Certificates are authenticated, issued, and managed by a trusted third party called a certification authority (CA).

Certificates are issued to all parties authorized to use HCAI Web services to send or receive data extracts. Insurer Users using the web application do not require a digital certificate. They log in on the web with a User Name and a password. The digital certificates are installed on the Insurer's integration server, which presents the certificate each time it connects to HCAI. Each digital certificate includes identification information about the connecting party and this information is the basis for authentication.

Web Services Authentication Errors

HCAI integration Web services authenticate the remote machine's information for each request message. If a requesting User cannot be authenticated, the system displays a Simple Object Access Protocol (SOAP) security error page.

HCAI authenticates its Users as follows:

Facility Users

Users representing Health Care Facilities use a Web log-in for authentication.

When Facilities access the application, they log in using unique User Names and passwords.

Health care Providers that offer services on behalf of more than one Facility require a separate User Profile for each Facility with whom they work..

Insurer Users

Users representing insurance companies use the Web log-in for authentication. When Insurer Users access the application, they log in using their unique User names and passwords.

Insurance companies that have HCAI integration over Web services for data feeds or data extracts require a client digital certificate in order to send or receive batch data. Digital certificates are issued to insurance companies for installation on each server integrating with HCAI.

HCAI Data Entry Centre, Help Desk, and Administrator Users

HCAI Users performing either helpdesk or administrative tasks use the Web login to access the system. Access to the system by application support staff is limited to a certain range of IP addresses, known to belong to authorized sources. This offers an additional layer of security, ensuring that these privileged accounts are restricted to only those individuals authorized by HCAI.

Authorization

HCAI enforces the specified privacy requirements by controlling User access to actions and data using a role based authorization framework. A User is permitted to perform a certain action or view a certain piece of information based on his or her role (a set of permissions necessary for a User to perform his or her job) and his or her domain (the specific companies, Facilities, Providers or Adjusters with whom the User is associated).

Users are assigned one or more roles that represent the operations they are allowed to perform in the system. A role contains one or more tasks. Tasks are the individual actions required to do a specific piece of work. Roles, and the tasks that are associated with them, define the range of actions that a User can perform. For example, one User may be able to match claimants to a claim but not be allowed to view or record decisions against the OCFs. This may be further qualified by specifying for which branch the User is allowed to perform the matching task. As mentioned above, this is accomplished by creating a domain, or organizational location, and limiting the User to operating within the domain.

HCAI domains, like roles, are specified at the User level. Users may be assigned one or more domains. For example, while a senior manager might have access to an entire organization, a branch manager might be allowed access to only one branch, and a unit manager or supervisor could have access to a number of Adjusters, or Adjuster teams.

Users will have access to only the organizations with which they are associated. This is managed by an HCAI Organization Administrator, within each Insurer, using HCAI's inherent authorization functionality. No Insurer will have access to another Insurer's information unless it is configured as an authorized company, as in a parent-child company relationship.

Authorization Configuration

Each Facility and Insurer organization must assign a designated administrator who is responsible for maintaining the organization's User information and authorization details. Administrators assign roles and domains to Users, specifying what they can do on the system.

It is the responsibility of the Insurer organization to ensure that Users are given access only to information that they are legally entitled to access.

HCAI limits authorization configuration permissions to the domain of the administrator. This means that an administrator within a particular organization is able to assign permissions only to Users associated with that organization.

Auditing

Auditing is the process of capturing and recording the significant actions performed by a User on the system, so that these actions can be reviewed and analyzed for security, privacy or other purposes.

The HCAI application has stringent auditing requirements because the system manages the personal health information of individual Claimants. Access to this information is rigorously controlled. Every attempt to access personal health information is recorded.

Audit logs for the monitored activities contain the following information:

- The identity of the User who performed the operation.
- The time of the activity.
- The type of activity, such as “Invoice submitted” or “Claim viewed.”
- The entity upon which the activity was performed, such as “OCF-21” or “OCF-23.”

All attempted actions are audited, regardless of whether the action is successful. All audit logging uses the HCAI Auditing Framework, a standard mechanism to record audit events consistently.

Audit Data Retrieval

Privacy laws require that personal health information be made available to individuals within 30 days of a request. HCAI is capable of providing the information necessary in order to comply with requests from individuals pursuant to existing privacy legislation.

Archiving

Information cannot stay in HCAI forever—eventually the accumulated data would impair system performance. HCAI includes processes for automatically archiving and purging data so that information that needs to be retained is archived and data that is no longer required can be deleted. Specific conditions must be satisfied before any HCAI data can be archived.

OCF Documents

- Plans and all related Invoices are treated as a single “OCF group”.
- Plans and all related Invoices are archived at the same time.
- Every Plan and related Invoice in the OCF group must be adjudicated.
- To qualify for archiving, one year must pass since the last adjudicated date for any Plan or Invoice in the OCF group.
- As noted in ***Chapter 5: Common Functionality***, archived OCFs are accessible through the HCAI web application via the OCF Document Search feature.

Claim and Claimant Information

- All the criteria for OCF document archiving must be met for a claim and claimant information in HCAI to be archived—in other words, all OCFs related to the Claim-Claimant file in HCAI must have already been archived.
- The Claim-Claimant file in question must be deactivated by the insurer.
- The Claim-Claimant file must have been deactivated (and remain inactive) for at least one calendar year.
- Archived Claim and Claimant information is not accessible through the HCAI web application but is however available through HCAI`s integration extract functionality.

Privacy Practices

HCAI has developed a comprehensive privacy program to guide employees, contractors and third parties in maintaining the confidentiality of PII. A Privacy Officer has been appointed to oversee, update and implement the program as well as acting as a resource to Users.

HCAI facilitates the transmission of data between Insurers and providers and does not collect the PII. For this reason, HCAI depends on the privacy practices of its Users to protect data when it is being entered into the system or is copied or stored outside the system.

HCAI expects Users to be aware of privacy practices that:

- outline your responsibility to protect the PII of your patients or claimants;
- ensure that the Authorizing Officer is familiar with the HCAI application and that access to Users in your organization is provided on a role-based model; as staff moves or leaves access is promptly changed or removed;
- comply with the requirements as set out in agreements signed with HCAI;
- require you to obtain and store the Claimant's consent as appropriate;
- outline the necessary information for treatment and payment;
- explain appropriate file access for your role;
- protect PII from unauthorized disclosure in paper, electronic or verbal format;
- ensure Claimant data is as accurate as possible;
- establish retention, storage and destruction guidelines for data not in the HCAI system;
- ensure your staff has privacy/security training on a regular basis and that changes in the HCAI system are communicated in a timely manner;
- ensure downloading Claimant data to a hard drive or mobile device is prohibited unless known to a supervisor; and
- outline the process in the case of a privacy breach in your organization.

Chief Privacy Officer
HCAI Processing
416- 644-3120
privacy@hcaiprocessing.ca